



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|--|-------------|----------------------|---------------------------------|-----------------------------|
| 10/702,167 | 11/05/2003 | Nancy Cam Winget | 72255/00006 | 7272 |
| 23380 | 7590 | 11/02/2007 | | |
| TUCKER ELLIS & WEST LLP 1150 HUNTINGTON BUILDING 925 EUCLID AVENUE CLEVELAND, OH 44115-1414 | | | EXAMINER DEBNATH, SUMAN | |
| | | | ART UNIT 2135 | PAPER NUMBER |
| | | | NOTIFICATION DATE 11/02/2007 | DELIVERY MODE ELECTRONIC |

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patents@tuckerellis.com
mary.erne@tuckerellis.com

| | | | |
|------------------------------|-------------------------------|-------------------------------|--|
| Office Action Summary | Application No. 10/702,167 | Applicant(s) WINGET ET AL. | |
| | Examiner Suman Debnath | Art Unit 2135 | |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 20 August 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-28 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-28 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-28 are pending in this application.
2. Claims 1, 9 and 17 are presently amended.
3. Claim 28 has been newly presented in the amendment filed on 20 August 2007.
4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office Action.

Continued Examination Under 37 CFR 1.114

5. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 08/20/2007 has been entered.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 17-25 and 27 are directed to a "computer program product" which could be a program/software/set of instructions. The examiner asserts that the limitation of the above claims raise a question as to whether or not the limitation actually claims the program. Moreover, independent claim 17 recites "A computer usable medium" in line 1.

Applicant's specification fails to define "a computer usable medium". Given the lack of a definition, Examiner interprets computer usable medium as characteristic of information that can be interpreted and acted on by a computer. Two types of information are referred to as computer-usable: bar codes, magnetic tape, magnetic-ink characters, and other formats that can be scanned in some way and read as data by a computer; and program code, the form in which instructions and data reach the computer's microprocessor. Media is defined as, the physical material, such as paper, disk, and tape, used for storing computer-based information. Media is plural; medium is singular. Given these interpretations, computer usable medium may be interpreted as including non-statutory embodiments such as machine code stored on paper. The above claims would have established a statutory category of the invention if the program recited in the above claims were stored on an appropriate medium and perform the function recited on the body of the claims when the program is read and executed by the computer/processor. However, the above claims are simply a computer program product which could be a software and thus do not clearly establish a statutory category of the invention. Therefore the claims are a program per se and don't fall within the statutory classes listed in 35 USC 101. The language of the claim(s) raises a question whether the Claim is directed merely to an abstract idea that is not tied to an environment or machine which would result in a practical operation producing a concrete, useful, and tangible result to form the basis of statutory subject-matter under 35 U.S.C. 101. (Warmerdam, 33 F.3d at 1360, 31 USPQ2d at 1759, 1760).

Claim Rejections - 35 USC § 102

7. Claims 1-28 are rejected under 35 U.S.C. 102(b) as being anticipated by Funk (Paul Funk; Simon Blake-Wilson; "draft-ietf-pppext-eap-tls-02.txt: EAP Tunneled TLS Authentication Protocol (EAP-TTLS)"; Internet-Draft PPPEXT Working Group; Nov. 2002, p. 1-40).

8. As to claim 1, Funk discloses a method of secure communication comprising: establishing a secure tunnel between first and second parties using an encryption algorithm that establishes an encryption key (Pages 9-10, section 4.3; Pages 11-13, sections 6-6.2);

authenticating the second party with an authentication server over the secured tunnel establishing an authentication key (Pages 9-10, section 4.3; Pages 11-13, sections 6-6.2 and Page 20, section 10);

verifying by the first party that the second party possess the same encryption and authentication keys as the first party (Pages 9-10, section 4.3; Pages 11-13, sections 6-6.2; and Page 20, section 10); and

provisioning a network access credential to the second party using the secured tunnel, responsive to the verifying the second party possess the same encryption and authentication keys as the first party ("The keying material is developed implicitly between client and TTLS server based on the results of the TLS handshake; the TTLS server will communicate the keying material to the access point over the carrier

Art Unit: 2135

protocol" —e.g. page 12-13, sections 6-6.2, see also Pages 9-10, section 4.3; Pages 11-16, section 6-7, Page 20, section 10).

9. As to claim 9 and 17, these are rejected using the same rationale as for the rejection of claim 1.

10. As to claims 2, 10 and 18, Funk discloses wherein the communication implementation between the at least first and second parties is at least one of a wired implementation and a wireless implementation (Pages 4-5, section 2).

11. As to claims 3, 11 and 19, Funk discloses wherein the encryption algorithm is an asymmetric encryption algorithm (Page 9-10; sections 4.2-4.3; Page 28, section 12).

12. As to claims 4, 12 and 20, Funk discloses wherein the asymmetric encryption algorithm is used to derive a shared secret, subsequently used in the step of establishing a secure tunnel (Page 9-10; sections 4.2-4.3; Page 28, section 12).

13. As to claims 5, 13 and 21, Funk discloses wherein the asymmetric encryption algorithm is Diffie-Hellman key exchange (Pages 36-37, section 14).

14. As to claims 6, 14 and 22, Funk discloses wherein the step of authenticating is performed using Microsoft MS-CHAP v2 (Pages 11-12; section 6; Pages 23-24, section 10.2.4).

15. As to claims 7, 15 and 23, Funk discloses further comprising a step of provisioning a public/private key pair on one of the at least first and second parties, and then to provision that public key on the respective remaining ones of the at least first and second parties (Pages 11-16, sections 6-7).

16. As to claims 8, 16 and 24, Funk discloses wherein the step of provisioning a public/private key pair comprises providing a server-side certificate in accordance with Public Key Infrastructure (PKI) (Pages 9-10, sections 4.2-4.3, Page 20, section 10).

17. As to claims 25, 26 and 27, Funk discloses wherein the verifying further comprises hashing the first party encryption key and the authentication key to produce a first hash ("...the master secret and random values" —e.g. Page 20-21 and Page 23); hashing the second party encryption key and the second party authentication key to produce a second hash; verifying the first and second hash are the same (Page 20-21 and Page 23, "the TTLS server must verify that the value of the MS-CHAP-Challenge AVP and the value of the Ident in the client's MS-CHAP-Response AVP are equal to the values generated as challenge material" —e.g. Page 23. Funk teaches the concept of hashing by using MS-CHAP-V2).

18. As to claim 28, Funk discloses further comprising invalidating a secure credential for the second party responsive to a failure of one of the group consisting of establishing the secure tunnel, authentication, and verifying second party has the same encryption and authentication keys ("If either item does not match exactly, the TTLS server must reject the client" –e.g. Page 23).

Response to Amendment

19. Applicant has amended claims 1, 9 and 17. See rejection above.

Response to Arguments

20. Applicant argues that: "Nowhere does Funk teach 1) that both parties verify their tunnel & authentication keys match the other party's nor providing a network access credential to the peer responsive to 1) successful establishment of the tunnel; 2) successful authentication; and 3) verifying keys each party acquired matching keys while establishing the tunnel and authenticating. Therefore, Funk does not disclose each and every element of independent claims 1, 9 and 17 and thus does not anticipate claims 1, 9 and 17 as currently amended."

Examiner maintains: Funk discloses both parties verify their tunnel and authentication keys match the other parties by using MS-CHAP-V2 challenge – response (e.g. page 20-23, EAP challenge uses security parameters as master secret,

client random and server random). Funk provides a network access credential to the peer responsive to 1) successful establishment of the tunnel; 2) successful authentication; and 3) verifying keys each party acquired matching keys while establishing the tunnel and authenticating (Funk discloses that the TTLS server (i.e. first party) distributes data connection keying information (i.e. provisions credentials) and other authorization information to the access point (i.e. second party) that carries the EAP-Success. —e.g. see page 13. Funk discloses that the keying material is developed based on the results of the TLS handshake; Funk uses MS-CHAP-V2 challenge — response to make sure both parties ensued same tunnel and authentication keys. — Page 23).

21: Examiner's note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant.

Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may be applied as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Conclusion

22. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See accompanying PTO 892.

- US 2005/0210251 A1-Linked authentication protocols.
- US 2002/0164022 A1-Method and apparatus for providing bus-encrypted copy protection key to an unsecured bus.
- US -2004/0081321 A1-Key agreement and transport protocol.

23. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Suman Debnath whose telephone number is 571 270 1256. The examiner can normally be reached on 8 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

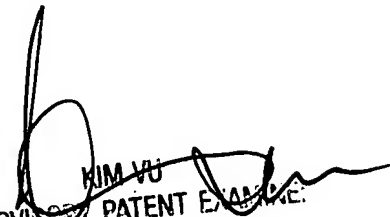
Application/Control Number: 10/702,167

Page 10

Art Unit: 2135

USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SD
SD


KIM VU
SUPERVISOR PATENT EXAMINEE
TECHNOLOGY CENTER 2100